Association for Information Systems
AIS Electronic Library (AISeL)

AMCIS 2010 Proceedings

Americas Conference on Information Systems (AMCIS)

8-2010

Strategic Role of Human Resource Management in Information Security Management

Kamphol Wipawayangkool
The University of Texas at Arlington, kamphol.wipawayangkool@mavs.uta.edu

Strategic Role of Human Resource Management in Information Security Management

Kamphol Wipawayangkool
The University of Texas at Arlington
kamphol.wipawayangkool@mavs.uta.edu

ABSTRACT

This paper overall aims to encourage researchers and managers to consider the role of human resource management (HRM) in the field of information security management (ISM) more seriously. This paper suggests that with more strategically active role of HRM through a combination of selection, training, and pay practices, organizations not only can manage people issues in ISM particularly security awareness and insider threats more effectively, but may be able to sustain competitive advantage of the organizations. This paper provides an initial framework and provokes thoughts on the topic for future researchers and practitioners in both ISM and HRM fields.

Keywords

Information security, strategic human resource management, sustainable competitive advantage.

INTRODUCTION

> *"The HR silo and the IT silo prevent good things from happening.… In my experience, HR hasn't really seen this insider-threat problem as their problem."* Ponemon, Chairman of the Ponemon Institute (Power, 2006)
>
> *"The greatest risk today is the insider."* Arrnette Heintze, Former Chief Security Officer for PepsiCo and Managing Partner of Hillard Heintze, a Chicago-based security consulting company (Power, 2006)

Rather than technology, people factors such as security awareness and insider threats are more significantly challenging to manage and are now considered more than ever to be fundamentally critical to the field of information security management (ISM) (Chang and Lin, 2007; Dhillon, 2007; Ruighaver et al., 2007; Schultz, 2004; Siponen, 2000; von Solms, 2001; von Solms and von Solms, 2004). As a result, it is unavoidable to acknowledge the potential role of human resource management (HRM) to ISM. Indeed, both the 2007 Deloitte Global Security Survey and 2007 Ernst & Young Global Information Security Survey suggest that it is crucial how an organization screens and employs people and that simple criminal background checks are not enough and that security training and awareness programs need to be emphasized and provided because how employees deal with information essentially represents risks. In short, since HR practices such as staffing and training appear to be very pivotal to ISM, it is more critical than ever to shift the role of HRM in organizations from traditionally seen as being passive to strategically active.

This paper contributes to the literature by attempting to link HRM with ISM theoretically, an attempt that has not been done much in prior literature. Nevertheless, this paper is not comprehensive in nature, but simply provides an initial framework and intends to provoke some thoughts on the topic for future researchers in either ISM or HRM field. This paper is organized as follows. First, literature background on ISM and HRM is discussed. Second, how HRM practices can help improve the ISM performance and may even help sustain the competitive advantages of organizations is discussed. Finally, implications are discussed.

LITERATURE BACKGROUND AND PROPOSITION DEVELOPMENT

Information Security Management

Information security management (ISM) fundamentally emphasizes confidentiality (to ensure privacy of information), integrity (to ensure authorized operations on information), and availability (to ensure availability of functional systems) (Dhillon, 2007). Technical aspects of ISM include computer software and hardware control concepts such as encryption and network security (Dhillon, 2007). Non-technical aspects cover topics such as risk management, culture management, and

regulatory compliance (Dhillon, 2007; Nosworthy, 2000; von Solms, 2001). As the field has grown, it is obvious that non-technical aspects as they are much related to people behaviors are far more challenging to manage and, costly if failed, than technical ones.

Among greatest risks in the field of ISM are insider threats (Humphreys 2008; Theohariduo et al. 2005) and security awareness (Jones, 2007; Kelly, 2006; Siponen, 2000; Straub and Welke, 1998; von Solms, 2001; von Solms and von Solms, 2004). First, insider threats refer to threats originating from people who can access corporate systems and abuse such privileges for personal gains. Such misbehaviors violate security protection of the firm and lead to losses of a combination of tangible and intangible assets. Second, according to the Information Security Forum (ISF) (2005), security awareness is defined as the extent to which organizational members understand the importance of information security, the level of security required by the organization and their individual security responsibilities, and act accordingly. Many incidents of security breaches could have been prevented if people are knowledgeable and aware of their actions.

A case in point that shows how people factors are critical to ISM is the explicit inclusion of human resource security controls in the ISO/IEC 27001 and 27002 (previously ISO/IEC 17799) (Humphreys, 2008; Theohariduo et al., 2005). They require that organizations establish HR practices such as conducting background and reference checks, requiring employees to sign confidentiality agreement, offering security awareness and training programs, and deleting all computer accounts associated with terminated employees. In sum, due to significant implications of people factors for ISM, the role of human resource management must be acknowledged and strategically planned to support ISM.

Strategic Role of Human Resource Management

Human resource management (HRM) refers to the uses of practices such as selection, training, and appraisal to manage people in organizations (Fombrum et al., 1984). Researchers increasingly suggest that those HR practices should be strategically integrated so that an organization can effectively utilize its human resources to achieve its strategic goals and ultimately to produce sustainable competitive advantage (Barney and Wright, 1998; Pfeffer, 2005; Wright and McMahan, 1992; Wright et al., 1994). Empirical studies also support such a view. For example, Huselid (1995) found that the complementarities among HR practices not only reduce employee turnover but also increase productivity and corporate financial performance. Macduffie (1995) found that plants that bundled HR practices with business strategy significantly perform better in both productivity and quality. Therefore, this paper suggests that if effective HR practices such as selection, training, and pay are strategically bundled with security policies, an organization will be able to manage its ISM more effectively and ultimately may be able to sustain its competitive advantages. Next, how HR practices can help organizations manage people issues in ISM more effectively is discussed.

Selection Practices

Selection practices refer to those organizational practices and activities used to identify and attract potential employees (Breaugh and Starke, 2000). Selection practices represent a gateway where potential employees enter organizations; thus, if executed effectively, selection practices can mitigate the risk of future security breaches exploited by individuals. The question is thus how. Among well known selection methods are general cognitive abilities, personality, biodata, and integrity tests (Hough and Oswald, 2000). As legal cases regarding key employees moving to work for competitors are eminent such as Microsoft vs. Google and Motorola vs. Zafirovski (Dulipovici and Baskerville, 2007), the ability of a selection method to predict intention to turnover is important (Barrick and Zimmerman, 2005). Interestingly, Barrick and Zimmerman (2005) found that job relevant biodata scales (i.e. tenure in a prior job, number of friends and family members in the focal organization, and employee reference), clear-purpose attitude and intention scales (i.e. intent to quit, and desire for a job), and disguised-purpose dispositional retention scales (i.e. self-confidence, and decisiveness) can predict individuals' intention to turnover even before they start working for the organization. Nonetheless, the intention to turnover may form after individuals work for a period of time; thus, integrity tests should also be employed to determine if intention to exploit information may be present. Schmidt and Hunter (1998) found that among a number of combinations of selection methods, using both general cognitive ability and integrity tests shows significantly high validity for predicting job performance. It implies that not only can the mixed method predict job-related performance, but personal integrity issues are also checked.

Essentially, this paper suggests that in order to mitigate the risk of insider threats more effectively, a combination of selection methods should be used. The ability to predict job performance, job-related learning, and other criteria, namely predictive ability (Schmidt and Hunter, 1998) of each method needs to be carefully evaluated so that such a combination can be effective.

Proposition 1a: Using multiple selection practices will help organizations mitigate the risk of insider threats more effectively.

Proposition 1b: Selection practices with high reliability and validity particularly in predicting intention to turnover will help organizations mitigate the risk of insider threats more effectively than those with low reliability and validity.

Training Practices

Training practices, particularly security training, can help organizations manage information security more effectively (Johnson, 2006; Kelly, 2006; Straub and Welke, 1998). According to the Gartner Group, nothing yields as much Return on Investment as security training and awareness (Schultz, 2004). Despite much investment in expensive advanced security systems, one could only imagine how much risk employees who naively handle sensitive information every day possess, if such information, which may be a source of competitive advantages of the organization, is transferred to competitors. Individuals must be trained how to handle information and become aware of possible consequences of their actions. Important topics for security training include motivating people to know more about information security in general and according to organizational security policies, promoting people to be cautious when handling information, and educating people how to recognize and avoid technical threats such as malicious software (Pabrai, 2005). Without security training designed to improve security awareness, people will always be the weakest link and organization will still be at risk (Bresz, 2004). In sum, if executed effectively, training practices can significantly improve employees' knowledge and awareness of information security issues.

Proposition 2a: Effective security training practices will improve employees' security awareness.

Thomson and von Solms (1998) highlighted that attitude can improve the effectiveness of security awareness programs. In training literature, job attitude has been found to influence how trainees perceive their training experiences, how they react to the training (Sitzmann et al., 2008; Tannenbaum et al., 1991), and the evaluation of effectiveness of the training program (Mathieu and Martineau, 1997, p. 205; Noe, 1986; Sahinidis and Bouris, 2008). One of the recent research models with strong prediction power ($r = 0.59$) is Harrison et al.'s (2006) attitude-engagement model which associates overall job attitude with individual effectiveness such as focal and contextual performance. In the model, job satisfaction and organizational commitment are the underlying dimensions of overall job attitude. Job satisfaction is defined as an emotional state resulting from the evaluation or appraisal of one's job experiences (Locke, 1970). Organizational commitment is defined as a feeling of sharing beliefs and values with one's entire organization (Meyer and Allen, 1991). If individuals feel satisfied with their job and are committed to the goals of organization, then they tend to have positive overall job attitude. Harrison and colleagues concluded that overall job attitude has considerable importance for understanding behavioral outcomes. Specifically, they stated that positive job attitude, which emerges from high level of job satisfaction and of organizational commitment, is likely to cause an individual to contribute desirable inputs to his or her work role. Much literature also appears to share the same views. Preining (1999) suggested that job satisfaction and commitment are likely to improve individual's security awareness. Sahinidis and Bouris (2008) found the significance correlation between employees' organizational commitment, job satisfaction, and motivation, and their perceived training effectiveness, which in turns will improve desired training outcomes.

Based on Harrison et al.'s attitude-engagement model, this paper suggests that overall job attitude, which is based on job satisfaction and organizational commitment, moderates the relationship between security training and security awareness in such a way that employees with positive overall job attitude attending security training will improve their security awareness rather than employees with negative overall job attitude. Thus, it is important for a training practice to maintain positive overall job attitude so that trainees' security awareness will be more effectively improved.

Proposition 2b: Overall job attitude will moderate the relationship between security training and security awareness improvement.

Pay Practices

"Money matters", if not directly, then indirectly through social influences. Pay refers to all forms of compensation, cash or non-cash (Williams et al., 2006). Pay satisfaction refers to overall positive or negative affect individuals have toward their pay (Williams et al., 2006). Based on their meta-analysis study, Williams et al. (2006) found that pay satisfaction essentially contributed by perceived fairness regarding pay level predicts job performance and job-related behaviors such as turnover, absenteeism, and intention to turnover. Similarly, Lee et al. (1999)'s two years study found that perceived justice of pay effectiveness on skill-based pay systems significantly affects positive individual outcomes. Such a relationship among perceived fairness of pay level, pay satisfaction, and individual performance is also expected to be found at team level. To

improve the visibility of fairness in team level reward systems, McClurg (2001) suggested that high level of communication from management to employees and employees' involvement in pay systems design and implementation should be present.

In sum, it is fair to infer that positive individual performance such as willingness to improve their security awareness can be expected if employees perceive their compensations to be fair and are satisfied with their pay levels. In addition, pay satisfaction may also mitigate the risk of insider threats as employees are satisfied with their pays and thus have no intention to turnover to potential competitors.

Proposition 3a: Effective pay practices will improve employees' pay satisfaction, which in turn will help organizations manage people issues more effectively. Specifically, pay satisfaction will moderate the relationship between selection practices and insider threats and the relationship between training practices and security awareness in such a way that high pay satisfaction will result in more stronger relationships.

Proposition 3b: Pay practices with high visibility of fairness will improve employees' pay satisfaction, which in turn will help organizations manage people issues more effectively, than those with low visibility of fairness.

Sustaining Competitive Advantage

In Barney (1991)'s Resource-Based View of the firm (RBV), value, rareness, inimitability, and non-substitutability determine the potential of the firm resources to produce sustainable competitive advantage. Firm resources include physical capital (e.g. technology), human capital (e.g. people and knowledge), and organizational capital resources (e.g. firm structure and management systems). Sustained competitive advantage exists when a firm implements "a value creating strategy not simultaneously being implemented by any current or potential competitors and when these other firms are unable to duplicate the benefits of this strategy" (Barney, 1991, p. 102). Applying the RBV to HR, Wright and McMahan (1992) suggested that HRM can indeed produce sustained competitive advantage because of the following reasons. Employees' knowledge and skills create values e.g. decreasing costs and increasing revenues. Some human resources particularly people with high ability are rare to find. Organizations' unique history and culture represent the inimitability of human resources. Finally, to achieve the status of non-substitutability, the resources should be strategically exploited, indicating the importance of managing HR practices as a bundle (Barney and Wright, 1998; Wright and McMahan, 1992). In sum, researchers suggest that strategic use of bundled HRM practices can produce sustained competitive advantage.

Based on the RBV and discussion above, this paper proposes that not only can each strategically active HR practice help organizations deal with ISM more effectively (that is, selection that can reduce insider threats (P1a, b) training practices that can improve employees' security awareness (P2a, b), and pay practices that maintain or improve employees' pay satisfaction (P3a, b)), but also a strategic combination of those practices may be able to produce sustainable competitive advantage of the organizations (P4). This paper is being cautious by using the term "leverage" for sustainable competitive advantage as seen in the model below, because it is arguable whether ISM alone can produce sustainable competitive advantage; rather, it may be more appropriate to suggest that ISM as a leverage can help organizations sustain their competitive advantage. Figure 1 depicts the research model along with the propositions.

Proposition 4: Effective people issues management contributed by strategically active role of HRM will produce leverage for sustainable competitive advantage.

IMPLICATIONS AND LIMITATIONS

Recognizing the significance of human factors in ISM, this paper contributes to security literature as the link between ISM and HRM is theoretically established through the RBV. This theoretical integration opens a number of future directions on studying the strategic role of HRM on ISM. The discussion in this paper is not comprehensive but simply intends to provoke some thoughts on the topic; thus, empirical studies to support the propositions developed in this paper are necessary. More detail on how each HR practice supports ISM and how there may be interaction effects among the practices (e.g. selection and training) are also needed. Finally, it is important to recognize that rather than HRM and ISM alone, other factors such as top management and leadership also play important role in producing both successful ISM and sustainable competitive advantage. For managers, it is time to turn around the passive role of HRM to the active one, given the pervasiveness of people factors in the security arena. In other words, in this information-sensitive era, HRM can no longer act as a paper work-processing unit in organizations, but it has to step up and strategically associate itself with ISM. As a result, effective collaboration among HR managers, IT managers, and top executive managers is needed.

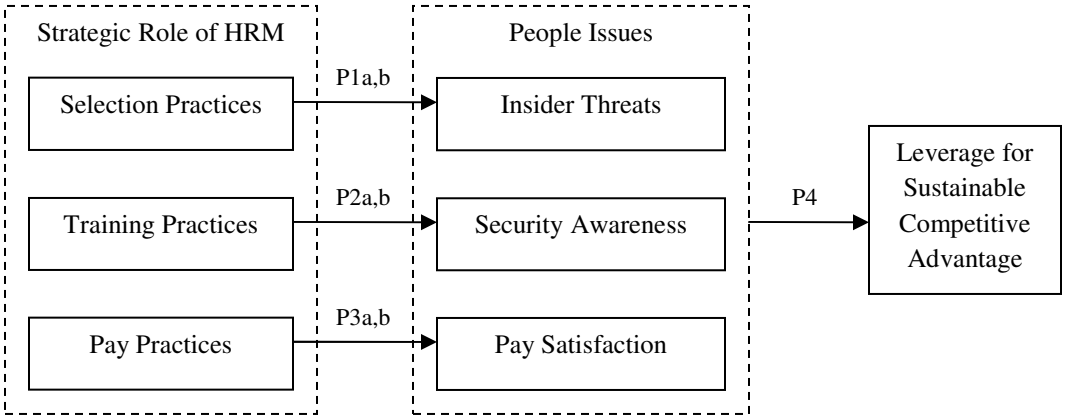

Figure 1. Strategic Role of HRM in ISM

CONCLUSION

Since people factors are considered more crucial than ever to the field of information security management (ISM), organizations should pay more attention to the role of human resource management (HRM). This paper overall suggests that with more strategically active role of HRM through an effective combination of selection, training, and pay practices, organizations not only can manage people issues in ISM more effectively, but also may be able to sustain the competitive advantage of the organizations.

REFERENCES

1. Barney, J. (1991) Firm resources and sustained competitive advantage, *Journal of Management*, 17, 1, 99-120.
2. Barney, J.B. and Wright, P.M. (1998) On becoming a strategic partner: the role of human resources in gaining competitive advantage, *Human Resource Management*, 37, 1, 31-46.
3. Barrick, M.R. and Zimmerman, R.D. (2005) Reducing voluntary, avoidable turnover through selection, *Journal of Applied Psychology*, 90, 1, 159-166.
4. Breaugh, J.A. and Starke, M. (2000) Research on employee recruitment: so many studies, so many remaining questions, *Journal of Management*, 26, 3, 405-434.
5. Bresz, F.P. (2004) People—often the weakest link in security, but one of the best places to start, *Journal of Health Care Compliance*, 57-60.
6. Chang, S.E. and Ho, C.B. (2006) Organizational factors to the effectiveness of implementing information security management, *Industrial Management & Data Systems*, 106, 3, 345-361.
7. Chang, S.E. and Lin, C. (2007) Exploring organizational culture for information security management, *Industrial Management & Data Systems*, 107, 3, 438-458.
8. Dhillon, G. (2007) *Principles of information systems security: Text and cases,* John Wiley & Sons, Inc.
9. Dhillon, G. and Backhouse, J. (2001) Current directions in IS security research: towards socio-organizational perspectives, *Information Systems Journal*, 11, 127-153.
10. Dulipovici, A. and Baskerville, R. (2007) Conflicts between privacy and property: The discourse in personal and organizational knowledge, *Journal of Strategic Information Systems*, 16, 187-213.
11. Fombrum, C., Tichy, N., and Devanna, M. (1984) *Strategic Human Resource Management*, Wiley, New York.
12. Harrison, D.A., Newman, D.A., and Roth, P.L. (2006) How important are job attitudes? Meta-analytic comparisons of integrative behavioral outcomes and time sequences, *Academy of Management Journal*, 49, 305-325.
13. Hough, L.M. and Oswald, F.L. (2000) Personnel selection: looking toward the future – remembering the past, *Annual Review of Psychology*, 51, 631-664.
14. Humphreys, E. (2008) Information security management standards: Compliance, governance, and risk management, *Information Security Technical Report*, doi: 10.1016/j.istr.2008.10.010
15. Huselid, M.A. (1995) The impact of human resource management practices on turnover, productivity, and corporate financial performance, *Academy of Management Journal*, 38, 3, 635-672.
16. Jones, D. (2007) Low cost security tools: Employee awareness, *Security*, November, 90-91.
17. Kelly, C.J. (2006) Awareness trumps new security toys, *Computerworld*, October, 44.

18. Lee, C., Law, K.S., and Bobko, P. (1999) The importance of justice perceptions on pay effectiveness: a two-year study of a skill-based pay plan, *Journal of Management*, 25, 6, 851-873.
19. Macduffie, J.P. (1995) Human resource bundles and manufacturing performance: Organizational logic and flexible production systems in the world auto industry, *Industrial and Labor Relations Review*, 48, 2, 197-221.
20. Mathieu, J.E., Martineau, J.W., (1997) Individual and Situational Influences on Training Motivation. In Ford, J.K, Kozlowski, S.W.J., Kraiger, K., Salas, E., and Teachout M.S (Eds.). *Improving Training Effectiveness in Work Organizations* (pp. 193-221), Lawrence Erlbaum Associates, Inc.
21. McClurg, L.N. (2001) Team rewards: how far have we come?, *Human Resource Management*, 40, 1, 73-86.
22. Meyer, J.P., and Allen, N.J. (1991) A three-component conceptualization of organization commitment, *Human Resource Management Review*, 1, 1, 61-89.
23. Noe, R.A. (1986) Trainees' attributes and attitudes: neglected influences on training effectiveness, *Academy of Management Review*, 11, 4, 736-749.
24. Nosworthy, J.D. (2000) Implementing information security in the 21st century – Do you have the balancing factors?, *Computers & Security*, 19, 337-347.
25. Pabrai, U.O.A. (2005) Awareness training: Strengthen your weakest link, *Certification Magazine*, August, 28-29.
26. Pfeffer, J. (2005) Producing sustainable competitive advantage through the effective management of people, *Academy of Management Executive*, 19, 4, 95-106.
27. Power, D. (2006) Companies Look to HR, IT Cooperation for Data Security, *Women's Wear Daily*, 10/2/2006, 192, 68.
28. Preining, W. (1999) Prevention of information loss: an overview of what can happen and some simple guidance on how to prevent it, *Technology, Law, and Insurance*, 4, 13-22.
29. Ruighaver, A.B., Maynard, S.B., and Chang, S. (2007) Organisational security culture: Extending the end-user perspective", *Computers & Security*, 26, 56-62.
30. Sahinidis, A.G., and Bouris, J. (2008) Employee perceived training effectiveness relationship to employee attitudes, *Journal of European Industrial Training*, 32, 1, 63-76.
31. Schmidt, F.L. and Hunter, J.E. (1998) The validity and utility of selection methods in personnel psychology: practical and theoretical implications of 85 years of research findings, *Psychological Bulletin*, 124, 2, 262-274.
32. Schultz, E. (2004) Security training and awareness-fitting a square peg in a round hole, *Computers & Security*, 23, 1-2.
33. Siponen, M.T. (2000) A conceptual foundation for organizational information security awareness, *Information Management & Computer Security*, 8, 1, 31-41.
34. Straub, D.W. and Welke, R.J. (1998) Coping with systems risk: Security planning models for management decision making, *MIS Quarterly*, 22, 4, 441-469.
35. Theohariduo, M., Kokolakis, S., Karyda, M., and Kiountouzis, E. (2005) The insider threat to information systems and the effectiveness of ISO17799, *Computers & Security*, 24, 472-484.
36. Thomson, M.E. and Von Solms, R. (1998) Information security awareness: Educating your users effectively, *Information Management and Computer Security*, 6, 4, 167-173.
37. Von Solms, B. (2001) Information Security – A multidimensional discipline, *Computers & Security*, 20, 504-508.
38. Von Solms, B and Von Solms, R. (2004) The 10 deadly sins of information security management, *Computers & Security*, 23, 371-376.
39. Williams, M.L., McDaniel, M.A., and Nguyen, N.T. (2006) A meta-analysis of the antecedents and consequences of pay level satisfaction, *Journal of Applied Psychology*, 91, 2, 392-413.
40. Wright, P.M. and McMahan, G.C. (1992) Theoretical perspectives for strategic human resource management, *Journal of Management*, 18, 2, 295-320.
41. Wright, P.M., McMahan, G.C., and McWilliams A. (1994) Human resources and sustained competitive advantage: a resource-based perspective, *International Journal of Human Resource Management*, 5, 2, 301-326.